

illegal wiretap activity and compromises, or suspected compromises, of lawfully authorized intercepts.

C. The Commission Should Specify That Carriers Are Not Required to Review the Substantive Basis or Underlying Legal Authority for Facially Valid Intercept Requests

46. Law Enforcement agrees with the Commission's statement in Paragraph 28 of the NPRM that there are at least two valid authorities for the implementation of an intercept: (1) a court order signed by a judge, and (2) a certification in writing by a law enforcement officer, as defined in 18 U.S.C. § 2510(7), that no court order is necessary pursuant to 18 U.S.C. § 2518(7). In addition, one party to a conversation can consent to the interception by law enforcement of the content of his or her conversations with another party (call content) or to the installation of pen register or trap and trace devices on his or her service. *See, e.g.*, 18 U.S.C. §§ 2511(2)(c) and 3121(b)(3). In such cases, the electronic surveillance statutes clearly indicate that no court order is required. Yet, instances have been reported of a carrier impermissibly refusing to provide the requested assistance in these circumstances, even where the proper subscriber consent has been presented.

47. It is not necessary for the Commission to adopt a rule that carriers include in their internal policies and procedures information provisions that would separately define the legal authorizations required for carriers to implement an intercept. In fact, carrier maintenance of such detailed authorization criteria could erroneously suggest to carrier personnel that they are entitled to substitute their review for that of a judge when a carrier is presented with a facially valid court order. Carriers are the implementers, not the enforcers, of lawful intercept orders or certifications under the electronic surveillance laws. The Commission should clarify that its rules do not purport to alter the electronic surveillance laws.

48. There are a number of specific points made in Paragraphs 28 through 31 of the NPRM concerning the requirements for electronic surveillance that warrant specific comment in order to ensure clarity. These points also illustrate the importance that Law

Enforcement attaches to the proposition that the Commission should not require carriers to be responsible for interpreting the subtleties of Federal or state electronic surveillance laws.

49. First, we offer the following to clarify what the Commission has suggested as the proper basis for “appropriate authorization” in cases of orders, exigent circumstances, and consent. It should be clarified that “appropriate legal authorization,” in cases of court orders, is not limited to those issues pursuant to 18 U.S.C. § 2518. For example, court orders also may be issued pursuant to the federal pen register and trap and trace statutes (18 U.S.C. §§ 3121, *et seq.*), analogous state law, and FISA. Hence, the discussion and emphasis placed exclusively on Title III law could well be confusing to carriers when discussing what constitutes “appropriate legal authorization.”

50. Second, as the Commission has correctly recognized, telecommunications carriers are obligated to implement interceptions based upon “certifications” under emergency circumstances (*see, e.g.* 18 U.S.C. § 2518(7); 18 U.S.C. § 3125; and 50 U.S.C. § 1805(e)). It should be noted, however, that these certifications (grounded in emergency circumstances) precede, rather than obviate the need for, court orders. The foregoing statutes make clear that within 48 hours (or less) after emergency interceptions are instituted, an appropriate court order must be filed with the court. When a law enforcement agency certifies to a telecommunications carrier that an emergency situation exists under the law, the telecommunications carrier is duty-bound to implement the interception effort. Neither CALEA nor any electronic surveillance law authorizes a telecommunications carrier to adjudge whether a statutory-based emergency exists or not. That is, carriers have no right to attempt to discern the factual or legal basis of the statutory emergency or to probe into which statutory category supports the emergency. Further, emergency authority and varying exigent circumstances related to emergency interceptions are found in a number of the electronic surveillance statutes, as discussed above, not just in Title III. Hence, Law Enforcement would recommend against the Commission’s proposal that carriers incorporate into their policies and procedures a “list of exigent circumstances found in 18 U.S.C. § 2518 (7).”

51. Third, the "consent" of a party to a communication (under Title III) or of a user (under the pen register/trap and trace statutes) is also recognized under the foregoing statutes as a basis for lawful authority to conduct interceptions (see e.g., 18 U.S.C. § 2511(2)(c) and 18 U.S.C. § 3121(b)(3)).

52. Law Enforcement would like to state, however, that it concurs with the Commission's tentative conclusion that existing laws adequately protect citizen's privacy and security rights against improper electronic surveillance. CALEA, at its core, focuses on the *preservation* of law enforcement electronic surveillance *capabilities* commensurate with, and pursuant to, the authority found in existing law, in a way consistent with communications privacy rights and security.

D. The Commission Should Ensure That Internal Carrier Authorizations and Procedures Are Designed to Maintain the Timeliness, Security, and Accuracy of Intercepts

53. Law Enforcement agrees with the Commission's proposal in Paragraph 30 of the NPRM to require carriers to designate specific employees to assist law enforcement officials in implementing lawful interceptions. Those personnel should be subject to the personnel procedures previously discussed. Moreover, Law Enforcement believes that there should always be at least one designated employee who is available to respond to appropriate law enforcement requests.

1. Designated Personnel.

54. For evidentiary and security reasons, Law Enforcement is greatly concerned by the Commission's suggestion in Paragraph 30 of the NPRM that non-designated employees be permitted to effect certain surveillance work. Law Enforcement strongly believes that only specifically designated carrier personnel should be permitted to have any involvement in, knowledge of, or access to an electronic surveillance or information concerning it. This

does not mean that only security personnel should be required for the installation of regular services, such as leased lines, to law enforcement, or that security personnel would be required to perform those functions from which it would be impossible even to infer that an intercept was involved.

55. Carriers must maintain records of all personnel who are involved in the installation and maintenance of intercepts. The reasons for maintaining such information include the fact that carrier personnel having any part in the installation of an intercept may be required to testify in a criminal prosecution as to how the intercept was installed and maintained. Without a clear "chain of custody" for the intercept, prosecutions might fail if law enforcement were unable to demonstrate Title III compliance.

56. Law Enforcement believes that all carrier functions involved in the installation or maintenance of an intercept should be implemented by designated personnel if, in the performance of any particular function, the carrier employee doing the work could acquire any knowledge, either express or implied, of the intercept. It is uncertain that a line could be drawn to isolate functions that could be performed by non-designated carrier personnel as part of their routine work assignments without those personnel becoming informed that the task at hand relates to a surveillance.

57. The procedures employed by any particular carrier pertaining to the issuance, assignment, and distribution of work orders must enable any such functions to be segregated in a secure way so that non-designated carrier personnel would be able to participate in a surveillance without knowing of that participation. Even the remote possibility that a non-designated employee might conclude that his work was in connection with a surveillance should be precluded. Otherwise, intercepts or the undercover accounts, identities, and locations used by many law enforcement agencies could be compromised if their existence were to become widely known.

58. Because all persons having knowledge of, or access to, all facets of an electronic surveillance must be accounted for, Law Enforcement believes that, for the security reasons stated above, only specifically designated carrier personnel should be permitted to have any involvement in effecting surveillance work where the function to be performed could enable such carrier personnel to know of the intercept. Carriers should be responsible for ensuring that any low-level tasks that might be identified as not requiring designated personnel are described, assigned, and performed in such a manner that no information is communicated from which the non-designated employee could even infer that an intercept is involved.

59. Law Enforcement also concurs with the Commission's general proposal in Paragraph 30 of the NPRM that only designated employees create records containing electronic surveillance information and that those records be kept separately. However, for the reasons stated above, Law Enforcement does not agree that a separate record keeping function performed by designated employees would be sufficient to eliminate the concerns posed by the prospect that non-designated employees could perform electronic surveillance functions.

60. In response to the Commission's request for comment, Law Enforcement offers the following with regard to the rules the Commission should consider in implementing Section 105 of CALEA. Such rules should specify—:

- Telecommunications carrier policies and procedures regarding designated (authorized) personnel, facilities, and security need to be in place and working in order to limit access to information concerning the existence of (including records concerning access and operation of) interception capabilities to those personnel authorized by the carrier. An audit trail regarding such information is also required.
- Carrier personnel designated to effect interceptions and to have access to information concerning interceptions must be carefully selected by a telecommunications carrier. A telecommunications carrier is, and should be,

responsible for ensuring that its designated personnel are trustworthy (e.g., have no serious criminal convictions, pending criminal charges, or bad credit history) and that they would be suitable for processing and handling sensitive law enforcement interceptions and information.

- An official list of a telecommunications carrier's designated personnel should be created and available at all times to appropriate, designated law enforcement personnel, for any operational needs and any necessary security review or checks that may be required. Such list should include the individuals' names, personal identifying information (date and place of birth, SSN), official titles, and contact numbers (telephone and pager). Nondisclosure agreements should be executed by such personnel.

As noted above, such trustworthiness determinations, and background checks are consistent with carriers' existing practice with regard to their Security Office personnel who handle and administer electronic surveillance orders.

2. Intercept Authorizations.

61. Law Enforcement believes, as stated earlier, that a court order or a certification (or a consent) is required before a lawful intercept may be implemented. It should be reiterated that a carrier's review of the legal process should be limited to confirming the order's or certification's facial validity and technical feasibility. The Commission may also wish to note that the presentation by telecopier of a facsimile copy of a court order or an emergency certification is sufficient service of process to trigger the carrier's obligation to respond. This is a particularly critical point in the case of larger carriers that have centralized security offices.

62. Law Enforcement also agrees with the Commission's proposal in Paragraph 31 of the NPRM that each carrier employee and officer who oversees interception activity be required to execute a document containing each of the items listed by the Commission in its

proposal, with one exception. Item 4 of the Commission's proposal should be deleted because it is impossible for carrier security personnel to know, in real time, when the interception must lawfully terminate.²⁵ To the extent that a carrier's burden might be lessened, it may be, however, that the execution of a certification would suffice in place of a more formal affidavit. In addition, Law Enforcement proposes that any such document have added to it an additional item stating that the signatory understands that unauthorized disclosure of intercept information is an actionable offense potentially subject to criminal or civil penalties, including imprisonment or fine, or both.

63. With respect to the first item on the list, the "telephone number(s) or the circuit identification number(s)," Law Enforcement believes that this category should be modified to include the telephone number(s) *and* the circuit identification number(s). This is the phrasing used by the Commission in connection with the record keeping requirement addressed in Paragraph 32 of the NPRM. In addition, Law Enforcement strongly urges the Commission to broaden the category to include the subscriber identifier(s) (IMSI or MIN number(s)) and the terminal identifier(s) (IMEI or ESN number(s)) that would apply to interceptions of wireless communications. These identifiers should be included because, in wireless networks, routing numbers and line identities may be insufficient to connect a particular telephone number to a specific subscriber.²⁶

64. Law Enforcement also appreciates that the paperwork burden on carriers should be minimized to the greatest extent possible, especially for large carriers or carriers that are involved in a substantial number of intercepts, while still maintaining all necessary safeguards. Law Enforcement wishes to ensure that the paperwork burden is never permitted to impede the timeliness with which intercept requests are implemented. The proposal that an affidavit or certification be prepared only by the employee or officer responsible for

²⁵ See *infra* note 26.

²⁶ IMSI numbers are "International Mobile Subscriber Identities;" MIN numbers are "Mobile Identity Numbers;" IMEI numbers are "International Mobile Equipment Identities;" and ESN numbers are "Electronic Serial Numbers." See Cellular Radio Telecommunications Intersystem Operations Signaling Protocols (Interim Standard), TIA/EIA/IS-41.5-C (February 1996).

overseeing the interception activity is, thus, supported. That document, however, should set forth the identities and functions of all carrier personnel who have knowledge of, or access to, information or facilities associated with the intercept. If, as Law Enforcement has suggested in its response to Paragraph 30 of the NPRM, each of those employees is a designated person, the individual personnel records of those individuals should contain the requisite certification concerning non-disclosure of intercept information.

3. Record Keeping.

65. In response to Paragraph 32 of the NPRM, Law Enforcement believes that ensuring the integrity of the records of electronic surveillance maintained by carriers is critical to the security and evidentiary concerns of Law Enforcement and the public safety.

66. Law Enforcement, therefore, concurs with the Commission's general proposal that carriers be required to keep records of the conduct of surveillance, and that those records be compiled contemporaneously with the start of each interception.²⁷ In addition, the Commission may wish to require the carriers to add the name of the issuing court in the case of a court order, which would assist both carriers and law enforcement in retrieving information when necessary. To ensure the integrity of the electronic surveillance effort, carriers should be required to maintain separate records of each surveillance activity, and those records should be maintained in a separate (including from FISA records) and secure storage area, access to which should be limited to a small number of designated carrier personnel.

²⁷ As an operational matter, the Commission should require that the actual initiation and termination of an electronic surveillance be manually effectuated by carrier personnel, rather than programmed into the switch beforehand. For example, even though Law Enforcement is authorized to conduct interceptions up to a 30-day period, it is required by law to terminate the interception sooner if the goals of the interception have been attained. Also, in a number of states, the 30-day interception period is computed beginning at 12:00 a.m. of the day on which the court signs an order, which would typically then lead to an interception being terminated at midnight. Such circumstances could lead to a problem if programming is exclusively relied upon in situations where, for example, an extension or emergency authorization may have been obtained before the expiration of the original order, but potentially after normal security office business hours (or where the order expires during a weekend). The presence of carrier personnel would provide assurance that there would be no interruption in a surveillance in such a circumstance.

67. It is essential to the admissibility of evidence that Law Enforcement be able to maintain these records for the same 10-year period required in 18 U.S.C. § 2518(8)(a). In that regard, Law Enforcement believes carriers should be required to transmit the originals, or certified original copies, of all electronic surveillance records to the cognizant law enforcement agency by no later than ten (10) days following the conclusion of an intercept. Law Enforcement understands that, while not necessarily required, carriers may wish to retain copies of those records. In such an event, the Commission should require that any records retained by a carrier after the originals or certified originals have been delivered to Law Enforcement be maintained in the same separate and secure manner as described above. Law Enforcement believes that these records are subject to the nondisclosure provision set forth in 18 U.S.C. § 2511(2)(a)(ii).

68. To the extent that a carrier has permitted a third party to have access to its switches or other facilities from which electronic surveillance could be detected, such carrier shall maintain records that will include the date, time, purpose, and identity of the third party personnel involved for each access permitted.²⁸

4. Timeliness.

69. As Law Enforcement has stated in its comments on the specific requirements addressed in Paragraphs 29–33 of the NPRM, one of the critical factors affecting the efficacy of electronic surveillance is the timeliness with which intercepts are implemented. This factor is a theme throughout the Commission’s discussion of carrier security policies and procedures. Section 103 of CALEA requires carriers to be capable of “*expeditiously* isolating, and enabling the government to intercept, all wire and electronic communications within that carrier’s network . . .” and “*rapidly* isolating, and enabling the government to

²⁸ For example, small carriers often have maintenance agreements with their manufacturers which could permit such activities to take place. In such cases, a carrier’s service contract may include such record keeping provisions.

access, call identifying information that is reasonably available to the carrier." 47 U.S.C. § 1002. The more cumbersome a carrier's implementation procedure, the greater the likelihood that investigations will be hampered by unnecessary delays.

70. Therefore, to facilitate the CALEA requirement that carriers respond promptly to interception orders and provide information "expeditiously" and "rapidly," the Commission should require that carriers receiving interception orders or certifications complete their internal approval and documentation process and implement the interception within 8 hours of receiving the court order, certification, or consent. For exigent circumstances, for example, in cases under 18 U.S.C. §§ 2518(7), 3125, no more than 2 hours should be allowed to elapse before an interception, pen register, or trap and trace is implemented. These time periods warrant the further requirement that carriers have a designated security officer and designated technical personnel available, either on duty or on call by pager, 24 hours a day, 7 days a week.

71. Law Enforcement also believes that the accelerated 2-hour time period that should apply to the duty of carriers to report compromises of intercepts to law enforcement should also apply to reporting intercept malfunctions following their discovery. As discussed above, the compromise of an intercept poses an immediate danger to the safety of any undercover personnel who may be involved in the investigation and perhaps to the subjects of the intercept as well. So too, malfunctioning intercepts can not only result in the loss of critical evidence, but also endanger public safety by inhibiting law enforcement's ability to respond in emergency circumstances. A time period longer than 2 hours would result in a needless waste of the law enforcement resources being dedicated to an inoperative electronic surveillance.

72. In Paragraph 33 of the NPRM, the Commission asks for comment on additional information that carriers should be required to provide to law enforcement. Law Enforcement believes carriers should be required to maintain and have accessible to Law Enforcement a point or points of contact available twenty-four (24) hours a day, seven (7)

days a week to ensure Law Enforcement access to the installation, monitoring, and maintenance of pen register, trap and trace, communications content, and other related electronic surveillance functions. Law Enforcement supports the efforts by the carriers and Commission to meet this obligation in the least burdensome manner possible.

E. No Distinction Is Made for Small Carriers Under CALEA

73. Law Enforcement strongly disagrees with the notion that CALEA contains any specific provision providing for the establishment of lesser requirements for small carriers insofar as their obligations concerning the implementation of CALEA's requirements is concerned. Nor do the electronic surveillance laws make such a distinction. From Law Enforcement's perspective, no sound policy reason exists for making a distinction between large and small carriers. Indeed, the assistance requirements set forth in the criminal statutes regarding electronic surveillance make it clear that law enforcement's ability to respond to important investigations, and frequently to life and death circumstances, cannot be dependent on the size of the carrier in the particular location where criminal activity may take place.

74. Law enforcement has no wish to burden small carriers unnecessarily, but the integrity and security of interceptions, and the impact that the loss of vital evidence may have on public safety and the successful conduct of criminal prosecutions, is unrelated to size. Under CALEA, a small carrier has the same obligation as a large carrier to respond to the dictates of the electronic surveillance laws and ensure that there are no unauthorized intercepts or disclosures of intercept information. There may be a practical correlation between the size of the carrier and the number of designated personnel that will be required by that carrier to fulfill its CALEA requirements. But new carrier entrants in critical geographic areas, even though they may be smaller, could conceivably receive a disproportionately large number of intercept requests.

75. Nonetheless, both Title III and CALEA apply across the board. Law enforcement's public safety and security concerns do not vary according to geography or

size. In the first instance, therefore, the CALEA regulatory requirements being developed by the Commission should be made to apply equally to all CALEA-covered entities, and a multi-tiered regulatory scheme, whether based on carrier revenues or number of subscribers, should be rejected by the Commission.

76. For these reasons, Law Enforcement disagrees with the proposal stated in Paragraph 35 of the NPRM to define a category of "small telecommunications carriers" based on \$100 million annual operating revenues. Likewise, Law Enforcement has several concerns about the Commission's proposal in Paragraph 35 to permit "small carriers" to elect to file a certification that its procedures are consistent with Commission rules regarding CALEA. Such a proposal likely would quickly become unworkable and, indeed, could lead to the imposition of an even greater administrative burden on carriers and the Commission.

77. Will penalties apply if a compliance certificate proves to be invalid due to the failure of an individual small carrier's policies and procedures to comply with Commission rules? Who would enforce the security policies, processes and procedures requirements in such cases? What safeguards for law enforcement would exist to ensure that intercepts could be implemented in a prompt, secure, and reliable manner while enforcement actions were pending? Would the Commission ultimately find itself in the position of providing detailed management and organizational directions to specific carriers? Furthermore, the \$100 million cutoff would effectively eliminate all but about 21 of the thousands of telecommunications carriers covered by CALEA from the more stringent regulatory requirements.²⁹

78. The Commission states in Paragraph 36 of the NPRM that smaller and newer carriers will be the least likely to be able to meet CALEA's requirements because they are unlikely to have the resources that are available to larger carriers. Law Enforcement does not believe this proposition necessarily withstands scrutiny. Rather, the resources necessary

²⁹ In 1994, approximately 21 local exchange carriers had revenues above \$100 million. See 1995 America's Network Directory (*citing* USTA 1994 Holding Company Report).

to develop procedures to comply with CALEA under the rules to be adopted in this proceeding are likely to be smaller for small carriers. It stands to reason that simpler procedures will be required for small carriers with less expansive or complex networks, fewer facilities, and smaller staffs. The expense of compliance likely to be borne by large carriers, whose networks cover more territory, offices, switches and staff, does not necessarily translate, dollar for dollar, to a small carrier whose personnel are likely to serve multiple functions in substantially simpler organizational bureaucracies.

79. In response to the Commission's request for proposals contained in Paragraph 36 of the NPRM, it should be clarified that CALEA's objectives extend far beyond law enforcement's mere ability to receive pen register, trap and trace, and interception services, upon request, from all carriers subject to CALEA. CALEA's objectives, at least in the context of security policies and procedures, include all of the ancillary protections discussed in the preceding comments by Law Enforcement that will ensure the timeliness, accuracy, security, and evidentiary integrity of those services and the information they produce. Moreover, laxity in following rules established by the Commission will ultimately lead to public harm because unlawful and unauthorized interceptions could more easily take place.

80. The Commission should not, directly or otherwise, take any action that results in small carriers, as defined according to some competition-based criteria or an arbitrary revenue cutoff, being relieved of their responsibilities under CALEA. Instead of instituting a certification procedure, which would be exceedingly difficult to monitor and lead to gaps in compliance, the Commission may wish to develop standardized forms to assist small carriers with compliance. These forms could be designed to elicit all the information that large carriers will be asked to provide. They could even be issued with a manual containing a template set of security policies and procedures, which the adoption of and adherence to could be deemed by the Commission to be CALEA compliant. But, should the Commission choose to pursue such a course to assist small carriers, the content of the forms and the manual should specifically be designed to ensure that identical standards are applicable to large and small carriers alike.

81. Law Enforcement would be willing to work with Commission staff to develop the appropriate forms, but wish again to emphasize that their primary concerns are that the timeliness, accuracy, security, and evidentiary integrity of surveillance information be protected. Beyond that, it may be more appropriate for the Commission, together with interested trade associations and individual carriers, to lead such an effort.

F. Commission Procedures

82. Law Enforcement agrees with the Commission's tentative conclusion in Paragraph 37 of the NPRM that 90 days from the effective date of the rules adopted in this proceeding is sufficient time within which the carriers should file their initial procedures with the Commission. Law Enforcement also agrees that the Commission's general rules concerning compliance with its rules are applicable to compliance with CALEA. The procedures and penalties in those rules should be applicable to all entities that are subject to CALEA. To the extent that, as part of an enforcement proceeding, the Commission requires production of records relating to electronic surveillance policies and procedures, it should take care to ensure that the security of law enforcement practices and methods is not compromised.

83. In the case of mergers or divestitures, Law Enforcement believes that statements concerning CALEA policies and procedures should be included with the applications filed with the Commission seeking license transfers and other prerequisite approvals before a merger or divestiture may be consummated. These statements should address how the affected carriers will implement requests for intercepts during any post-transaction period preceding a consolidation or divestiture. Following the Commission's approval of a transaction, the surviving entity, in the case of a merger, or the new owner, in the case of a divestiture, should then have 90 days within which to file with the Commission any modifications to its procedures.

84. For reasons stated previously regarding the definition of telecommunications carrier, Law Enforcement concurs with the Commission's tentative conclusion in Paragraph 38 of the NPRM that the rules promulgated in this proceeding should apply to all telecommunications carriers, as defined by CALEA. To the extent that future determinations of substantial replacement, or the advent of new services, result in additional entities being included under the CALEA definition of telecommunications carrier, the rules should immediately become applicable to those entities.

VI. JOINT BOARD

85. The NPRM issued by the Commission to address cost recovery issues for non-reimbursed CALEA expenditures was issued in connection with the Federal-State Joint Board convened pursuant to Section 229(e)(3) of the Communications Act to consider changes to the Commission's Part 36 and Part 21 rules related to charges, practices, classifications, and regulations for cost recovery in light of CALEA. Law Enforcement believes that the Commission should use its current methodologies, to the fullest extent possible, for making determinations on how non-reimbursed CALEA costs should be allocated. Law Enforcement will comment in the separations proceeding in the event that submissions from other interested parties require further comment.³⁰

VII. ADOPTING TECHNICAL STANDARDS

86. Law Enforcement concurs with the Commission's stated intention in Paragraph 44 of the NPRM not to address in this proceeding the issues raised in the petition by the Cellular Telecommunications Industry Association ("CTIA") regarding the technical standard for assistance capability envisioned by CALEA. The Commission is to be applauded for urging law enforcement and industry to continue their efforts to develop the necessary requirements, protocols, and standards.

³⁰ See *Jurisdictional Separations Reform and Referral to the Federal-State Joint Board*, CC Docket No. 80-286 (released October 7, 1997).

87. Law Enforcement has the following specific comments on the points made by the Commission in its description of the standards issue set forth in Paragraphs 41 through 43 of the NPRM. In Paragraph 41, it should be clarified that the obligation to consult on standards issues falls equally on the Justice Department, carriers and manufacturers. *See* 47 U.S.C. § 1005 (manufacturers) and 47 U.S.C. § 1006 (Justice Department and carriers).³¹ In addition, it should be noted that, although carriers may be deemed to be in compliance with CALEA if they comply with publicly available technical requirements, the technical requirements must meet the capabilities set forth in Section 103 of CALEA. The electronic surveillance requirements under Section 103 of CALEA and the underlying electronic surveillance statutes are not subject to modification by carriers. Rather, technical requirements contained in an industry standard should concern only the means by which those electronic surveillance requirements are to be met.³²

88. Law Enforcement believes that the promulgation of technical requirements or standards to implement the assistance capability requirements of the CALEA is vital to the preservation of law enforcement's electronic surveillance capability in an ever-changing telecommunications environment. Law Enforcement further believes that CTIA's industry consensus document proposing a standard (Standards Proposal [SP] 3580A) is technologically deficient because it lacks certain requisite functionality to fully and properly

³¹ Manufacturers and support services providers "have a critical role in ensuring that lawful interceptions are not thwarted." H.R. Rep. 103-827, 103d Cong., 2d Sess., at 26 (October 4, 1994).

³² We would like to clarify the Commission's statement in the NPRM (the Commission states: "[w]ith respect to information acquired solely through pen registers or trap and trace devices, the call-identifying information cannot include any information that may disclose the physical location of the subscriber, except to the extent that the location may be determined by the telephone number alone.") *See* NPRM, ¶¶ 7 and 40. The CALEA section to which the Commission is referring, Section 103(a)(2), in fact contains language that specifies that location-related call-identifying information may not be acquired by law enforcement "solely pursuant to the authority for pen registers and trap and trace devices . . ." The distinction is that the CALEA constraint involved is not one tied to the use of the device or the equipment, but rather to the *legal authority required to be provided*. CALEA Section 103(a)(2) specifies that the legal authority cannot be that set forth solely under the federal pen register and trap and trace statutes. Location-related call-identifying information can be lawfully acquired by Federal authorities by *other* legal authority (e.g., Title III, the court order specified in 18 U.S.C. § 2703(d), or a search warrant, etc.). This is an important distinction both legally and operationally. Aside from the legal authority specified to acquire location-related call-identifying information noted above, law enforcement recognizes, especially in kidnaping and extortion cases, that operationally the location of the kidnapper or extortionist (and the hostage victim) is often of prime or singular importance -- more important, for example, than intercepting the content of the criminal's communication.

conduct lawful electronic surveillance. Law Enforcement had proposed amendments to SP-3580A to include additional functionalities, thereby creating a technical standard that would fully meet the assistance capability requirements of Section 103 of CALEA and satisfy the investigative, operational, and evidentiary needs of law enforcement. Because this is an ongoing process, which the Commission acknowledges, Law Enforcement concurs that it would be inappropriate to address these issues in this proceeding.³³

89. Congress believed it beneficial to use “publicly available technical requirements or standards adopted by an industry association or standard-setting organization . . . to *meet* the [assistance capability] requirements of Section 103” (emphasis added). To give impetus to such efficient and industry-wide standards efforts, Congress offered a so-called “safe harbor” to those carriers, manufacturers, and support service providers that comply with publicly available standards or technical requirements that fully meet the statutory mandates of Section 103.

90. Carrier compliance with the assistance capability requirements of Section 103 is required whether or not industry-wide technical requirements or standards are actually used, or ever promulgated. The “safe harbor” provision applies only where the technical requirements or standards *fully meet* the assistance capability requirements of Section 103.

VIII. REQUESTS UNDER THE REASONABLY ACHIEVABLE STANDARD

91. At Paragraphs 45 through 48 of its NPRM, the Commission requests comments on “Requests Under the ‘Reasonably Achievable’ Standard.” Under Section 109 of CALEA, telecommunications carriers or any other interested party may petition the Commission to determine whether compliance with the assistance capability requirements of CALEA Section 103 is reasonably achievable with respect to equipment, facilities, or services

³³ On December 5, 1997, Telecommunications Industry Association and Alliance for Telecommunications Industry Solutions published an interim standard, J-STD-025, entitled Lawfully Authorized Electronic Surveillance.

installed or deployed after January 1, 1995. CALEA sets forth a number of factors the Commission must take into consideration when making its determination regarding whether compliance is reasonably achievable. Law Enforcement believes that these factors need to be weighed and applied in light of the critical importance to public safety of preserving law enforcement's electronic surveillance capabilities in a modern, mobile, information-based, and communications-driven society.

92. Before commenting directly on the Commission's request for comment on this issue, Law Enforcement wishes to note two sources of potential misunderstanding in these paragraphs. First, at footnote 155, the Commission states "Equipment, facilities, and services deployed on or before January 1, 1995 need not comply with the capability requirements of Section 103." While it is true that such equipment, facilities, and services will be "grand fathered" if the Attorney General chooses not to reimburse carriers for the necessary modifications, it is more appropriate to state that these equipment, facilities, and services will be deemed to be in compliance with CALEA until such time as the Attorney General agrees to reimburse or until a significant upgrade or major modification is made. At that point, the equipment, facilities and services will have to meet the requirements of Section 103 of CALEA.

93. Additionally, Paragraph 47 of the Commission's NPRM discusses reimbursement for meeting the capacity requirements set forth in accordance with Section 104 of CALEA. Law Enforcement wishes to note that the reasonably achievable standard of CALEA does not apply to capacity compliance or reimbursement; rather, it applies solely to compliance with the assistance capability requirements of CALEA Section 103. This distinction is made clear in CALEA.³⁴

³⁴ The Commission (in footnote 163) characterizes the FBI's capacity requirements as based on a "percentage of engineered capacity." Although the FBI issued its *Initial Notice of Capacity* that expressed future estimated actual and maximum capacity requirements in terms of "percentage of engineered capacity", after full consideration of all submitted comments, the FBI issued a *Second Notice of Capacity* that expressed future estimated actual and maximum capacity requirements in terms of geographically-based numbers of communications content, pen registers, and trap and trace devices. Neither the *Initial* nor *Second Notice of Capacity* was initiated under a rulemaking proceeding. See *Implementation of the Communications Assistance for Law Enforcement Act, Second Capacity Notice*, 62 Fed.Reg. 1902 (1997).

94. With regard to petitions for determinations of reasonable achievability, Law Enforcement suggests the following procedural requirements. First, because cost will clearly play a significant role in the Commission's determinations, Law Enforcement suggests that the Commission require that individual carrier petition submissions include an estimate of the reasonable costs directly associated with the modifications under consideration. The showing should be required in the initial carrier petition in order to provide the Commission (and the Attorney General through notice from the Commission) with the information necessary to its determination at the initial stage of the process. Further, requiring such a showing will also allow the Attorney General to make a prompt decision regarding reimbursement of additional reasonable costs in the event that the Commission determines that some, or all, of the costs associated with necessary modifications are not reasonably achievable.

95. Law Enforcement also requests that the Commission present its determinations in terms of dollar amounts. Specifically, should the Commission determine that a modification is not reasonably achievable, Law Enforcement suggests that the Commission make the further determination as to what portion of the costs are reasonably achievable for the carrier. Again, presenting the Commission's findings in this manner will expedite the Attorney General's decisions regarding reimbursement of additional reasonable costs. Should the Commission state only that a modification is or is not reasonably achievable without addressing the issue of which costs should be assumed by the carrier, and which costs should be considered for reimbursement by the Government, the CALEA implementation process will be significantly delayed.

96. With respect to the factors listed in Paragraph 45 of the NPRM, Law Enforcement believes that the first factor on the list in Paragraph 45 pertaining to the effect of compliance on public safety and national security should be deemed to be the paramount consideration in the Commission's determination of reasonable achievability. CALEA states in its preamble that it is an act "to make clear a telecommunications carrier's duty to

cooperate in the interception of communications for law enforcement purposes." *Id.* This clear expression of legislative policy should inform the Commission's decision on how each of the statutory factors is weighted and applied to requests pertaining to reasonable achievability. This process should be conducted on a case-by-case basis.

IX. EXTENSIONS OF COMPLIANCE DATE

97. Law Enforcement concurs with the Commission's decision in Paragraph 50 of the NPRM to not promulgate specific rules regarding requests for extensions of time to comply with CALEA in this proceeding. With respect to the Commission's proposal to consider petitions for extensions of time on the basis of the criteria specified in Section 109 to determine if it is reasonably achievable for a carrier, for "any equipment, facility, or service installed or deployed after January 1, 1995" to comply with the assistance capability requirements of Section 103 of CALEA, it should be noted that the issue of reasonable achievability requires consultation with the Attorney General. In this regard, it may be that the different issues presented by the question of whether an extension should be granted and the question of whether reimbursement is required might require a significantly different weighing of the reasonable achievability factors set forth in Section 109 of CALEA.

98. For example, development, manufacturing, and deployment schedules in the industry might lead to a request for extension on grounds of reasonable achievability. The grant of such a request would not necessarily mean that compliance with the assistance capability requirements of Section 103 of CALEA is not "reasonably achievable" under Section 109 such that the Attorney General would be required to reimburse a carrier lest it be "deemed" to be in compliance with CALEA under Section 109(b)(2)(B).

99. The former is an issue of timing; the latter is an issue of technical capability. It should also be noted that there may also be network-based, or other non-switch-based, solutions that would enable a carrier to provide certain surveillance services to law enforcement under Section 103 of CALEA that would preclude the grant of an extension.

Law Enforcement looks forward to working with the Commission and industry on the development of applicable rules in both circumstances.

X. REPORTING AND RECORD KEEPING

100. Law Enforcement agrees in part with the Commission's tentative conclusion that some carriers may have in place practices for proper employee conduct and record keeping. However, Law Enforcement also believes that the different approaches to electronic surveillance presupposed by CALEA, that is, switch- or network-based solutions, may render these existing procedures inadequate.

101. In the past, for example, a director of carrier security, pursuant to legal process, might advise law enforcement of the line appearance and cable and pair information necessary for an intercept. Law enforcement technical personnel would actually implement the intercept. In the future, CALEA solutions, which may be largely switch- or network-based, contemplate more extensive and direct involvement by carrier personnel. As a result, the manner in which interceptions are conducted and the number of carrier personnel involved may be substantially different. Consequently, even for carriers with whom law enforcement has worked in the past, there may need to be an increase in the level of attention paid to designated carrier personnel and their activities regarding interceptions, as well as an enhanced level of record keeping. It may be that carriers with extensive experience in working with Law Enforcement in this area will be able to make these procedural and management changes more easily than others.

XI. CONCLUSION

102. Law Enforcement urges the Commission to adopt a fair, balanced, and reasonable approach to the requirements of CALEA that is consistent with the Act's overall purpose of preserving law enforcement's electronic surveillance capabilities in today's technologically advanced U.S. telecommunications markets. Congress understood that the

need for the expeditious and rapid delivery of surveillance information would be critical to the fulfillment of Law Enforcement's public safety mandate. The accuracy, security, and evidentiary integrity of that information must also be safeguarded and ensured for it to be effectively used in criminal prosecutions.

103. Law Enforcement urges the Commission to keep the purpose of CALEA in mind:

to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, feature and services.³⁵

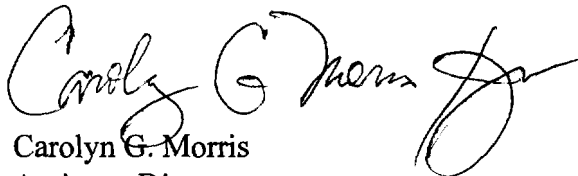
The proposals and suggestions in these comments meet the interests of Law Enforcement in ensuring the security, accuracy, integrity, and timely effectuation of electronic surveillance. The comments offered by Law Enforcement regarding the definitions presented by the Commission in this NPRM will likewise enable Law Enforcement to keep pace with rapidly advancing technology in today's telecommunications markets.

³⁵ H.R. Rep. 103-827, 103rd Cong., 2d Sess., at 9 (October 4, 1994).

104. None of the proposals, suggestions, and definitions in these comments, if they are adopted by the Commission, will impede the development and introduction of new technologies. Nor will their adoption unduly burden the service provider community. Moreover, none of the proposals, suggestions, and definitions in these comments will adversely impact the communications privacy or security of the public. Indeed, they should enhance communications privacy and security. The Commission's ongoing role in fulfilling the fundamental public safety purposes of CALEA is critical, and Law Enforcement appreciates the Commission's efforts in this matter.

Respectively submitted,

FEDERAL BUREAU OF INVESTIGATION

A handwritten signature in black ink, appearing to read "Carolyn G. Morris". The signature is fluid and cursive, with a large, stylized "C" at the beginning and a long, sweeping flourish at the end.

Carolyn G. Morris
Assistant Director
U.S. Department of Justice
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Rozanne R. Worrell
Rozanne R. Worrell

**IN THE MATTER OF
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT
CC DOCKET NO. 97-213
SERVICE LIST**

***The Honorable William E. Kennard, Chairman
Federal Communications Commission
1919 M Street N.W. - Room 814
Washington, D.C. 20554
202-418-1000**

***The Honorable Harold Furchtgott-Roth, Commissioner
Federal Communications Commission
1919 M Street N.W. - Room 802
Washington, D.C. 20554
202-418-2000**

***The Honorable Susan Ness, Commissioner
Federal Communications Commission
1919 M Street N.W. - Room 832
Washington, D.C. 20554
202-418-2100**

***The Honorable Michael Powell, Commissioner
Federal Communications Commission
1919 M Street, N.W. - Room 844
Washington, D.C. 20554
202-418-2200**

***The Honorable Gloria Tristani, Commissioner
Federal Communications Commission
1919 M Street, N.W. - Room 826
Washington, D.C. 20554
202-418-2300**

*** A. Richard Metzger, Chief, Common Carrier Bureau
Federal Communications Commission
1919 M Street N.W. - Room 500B
Washington, D.C. 20554**